UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

FORTINET, INC.,

Plaintiff,

v.

FORESCOUT TECHNOLOGIES, INC.,

Defendant.

Case No. 20-cv-03343-EMC

ORDER DENYING PLAINTIFF'S MOTION TO DISMISS COUNTERCLAIMS

Docket No. 115

I. INTRODUCTION

In this action, Defendant Forescout Technologies, Inc. ("Forescout") counterclaims against Plaintiff Fortinet, Inc. ("Fortinet"), alleging that Fortinet infringed six of its patents and tortiously interfered with its business relations.

Pending before the Court is Fortinet's motion to dismiss Forescout's counterclaim. Fortinet argues that four of Forescout's patents claimed ineligible subject matter under 35 U.S.C. § 101 and that Forescout's claim for tortious interference should be dismissed due to: (1) lack of subject matter jurisdiction, (2) federal law preemption of the state claim, and (3) failure to state a plausible claim. For the following reasons, the Court **DENIES** Fortinet's motion to dismiss.

A. Factual Background

Fortinet sells cybersecurity products, software, and services to large institutional customers. Docket No. 67 at 1. Forescout is a competitor of Fortinet in the cybersecurity market and owns U.S. Patent No. 8,590,004 ("the '004 Patent") (Method and System for Dynamic Security Using Authentication Server); Patent No. 10,652,116 ("the '116 Patent") (Device Classification); Patent No. 10,530,764 ("the '764 Patent") (Post-Connection Client Certificate

Authentication); Patent No. 6,363,489 ("the '489 Patent") (Method for Automatic Intrusion Detection and Deflection in a Network); and Patent No. 10,652,278 ("the '278 Patent") (Compliance Monitoring). Counterclaim at 53, 55, 57, 60.

On February 9, 2020, Forescout publicly announced a major acquisition in which Advent International ("Advent"), a global private equity investor, would acquire all outstanding shares of Forescout. *Id.* at 43. One business day before Advent was scheduled to close the acquisition, Fortinet filed its Complaint, then allegedly engaged in a campaign to smear Forescout. *Id.* Fortinet allegedly told CRN, an industry news source, that Fortinet:

> **[D]oesn't take litigation lightly** and has only engaged in lawsuits to protect its intellectual property on seldom occasions when it is left no alternative. But Forescout's **wrongful incorporation** of Fortinet's intellectual property into its product offerings is **material and goes to the heart of Fortinet's business**.

Id. at 46.

Forescout further alleges that Fortinet falsely raised doubts on Forescout's financial solvency to "existing and potential customers." *Id.* Fortinet's major accounts manager distributed a sample email used to "target folks looking at or using ForeScout," which stated the following:

> With (insert company name) 's up and coming investment in (insert NAC, zero trust security, whatever way you would like to describe the project) I wanted to **insure you were aware of the ongoing legal problems** and future of Forescout. In short, Fortinet **has filed lawsuit against Forescout for patent infringement related to technology held within FortiNAC**. Their acquisition by Advent and bid to be taken private was put on hold resulting in Forescout now filing a lawsuit against Advent, all **this leaving Forescout on uncertain ground financially**. This information is **all public and can information on it is readily accessible**." – From here, you **could include any of the various links to articles detailing the situation with Forescout, the financial comparison**, or any other info you think would resonate. Below are some [links to articles about Forescout's legal problems caused by Fortinet][.]

Id. at 46–47.

B. Procedural Background

Fortinet alleged infringement of three patents in its original Complaint and two additional patents in its Amended Complaint. Docket No. 1; Docket No. 67. In November 2020 and June 2021, the Court granted in part and denied in part Forescout's motions to dismiss which argued

that the patents claimed ineligible subject matter and were, therefore, invalid under § 101. Docket No. 24; Docket No. 71.

In July 2021, Forescout brought counterclaims against Fortinet, alleging infringement of six patents, as well as a claim for tortious interference based on extrajudicial statements made by Fortinet. On August 17, 2021, Fortinet moved to dismiss the counterclaims, including the '116, '764, '489, and '278 Patents.

II. LEGAL STANDARD

The Federal Rule of Civil Procedure 8(a)(2) requires a complaint to include "a short and plain statement of the claim showing that the pleader is entitled to relief." Fed. R. Civ. P. 8(a)(2). A complaint that fails to meet this standard may be dismissed pursuant to the Federal Rule of Civil Procedure 12(b)(6). *See* Fed. R. Civ. P. 12(b)(6). To overcome a Rule 12(b)(6) motion to dismiss after the Supreme Court's decisions in *Ashcroft v. Iqbal*, 556 U.S. 662 (2009), and *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 127 (2007), a plaintiff's "factual allegations [in the complaint] 'must . . . suggest that the claim has at least a plausible chance of success." *Levitt v. Yelp! Inc.*, 765 F.3d 1123, 1135 (9th Cir. 2014). The court "accept[s] factual allegations in the complaint as true and construe[s] the pleadings in the light most favorable to the nonmoving party." *Manzarek v. St. Paul Fire & Marine Ins. Co.*, 519 F.3d 1025, 1031 (9th Cir. 2008). However, "allegations in a complaint . . . may not simply recite the elements of a cause of action [and] must contain sufficient allegations of underlying facts to give fair notice and to enable the opposing party to defend itself effectively." *Levitt*, 765 F.3d at 1135. "A claim has facial plausibility when the plaintiff pleads factual content that allows the court to draw the reasonable inference that the defendant is liable for the misconduct alleged." *Ashcroft*, 556 U.S. at 678. "The plausibility standard is not akin to a probability requirement, but it asks for more than a sheer possibility that a defendant has acted unlawfully." *Id.*

III. DISCUSSION

A. Patent Subject Matter Eligibility Under § 101

Under the Patent Act of 1952, patents are "presumed valid." 35 U.S.C. § 282(a). "As such, an alleged infringer asserting an invalidity defense pursuant to § 101 bears the burden of

proving invalidity by clear and convincing evidence." *Cisco Sys., Inc. v. Uniloc USA, Inc.*, 386 F. Supp. 3d 1185, 1190 (N.D. Cal. 2019) (citing *Microsoft Corp. v. I4I Ltd. P'ship*, 564 U.S. 91, 95, 131 (2011)). "Patent eligibility under 35 U.S.C. § 101 is ultimately an issue of law" but "may contain underlying issues of fact." *Berkheimer v. HP Inc.*, 881 F.3d 1360, 1365 (Fed. Cir. 2018). "Like other legal questions based on underlying facts," patent eligibility "may be, and frequently has been, resolved on a Rule 12(b)(6) or (c) motion where the undisputed facts . . . require a holding of ineligibility under the substantive standards of law." *SAP Am., Inc. v. InvestPic, LLC*, 898 F.3d 1161, 1166 (Fed. Cir. 2018). Thus, "[a]lthough claim construction is often desirable, and may sometimes be necessary, to resolve whether a patent claim is directed to patent-eligible subject matter," it is not "an inviolable prerequisite to a validity determination under § 101," and may be eschewed "[w]here the court has a full understanding of the basic character of the claimed subject matter." *Voip-Pal.Com, Inc. v. Apple Inc.*, 375 F. Supp. 3d 1110, 1124 (N.D. Cal. 2019).

Section 101 defines the scope of patent-eligible subject matter. It provides: "Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor." 35 U.S.C. § 101. Patents may not be obtained for "laws of nature, natural phenomena, [or] abstract ideas." *Alice Corp. Pty. v. CLS Bank Int'l*, 573 U.S. 208, 217 (2014). In *Alice*, the Supreme Court established a two-step test that district courts must apply in a patent eligibility analysis under §101.

At step one, the court must "determine whether the claims at issue are directed to a patent-ineligible concept," i.e., a law of nature, natural phenomenon, or an abstract idea. *Id.* at 218. If so, then the court moves to step two, which "consider[s] the elements of each claim both individually and 'as an ordered combination' to determine whether [any] additional elements 'transform the nature of the claim' into a patent-eligible application" of the ineligible subject matter. *Id.* at 217 (quoting *Mayo Collaborative Servs. v. Prometheus Lab'ys, Inc.*, 566 U.S. 66, 78–79 (2012)).

While the precise contours of what constitutes an "abstract idea" under step one remains elusive, the Supreme Court has identified algorithms, mathematical formulae, "fundamental economic practice[s] long prevalent in our system of commerce," and other "method[s] of

organizing human activity" as impermissibly abstract. *Alice*, 573 U.S. at 218–20 (citing *Bilski v. Kappos*, 561 U.S. 593, 599 (2010)). To determine whether the claims at issue are directed to one of those patent-ineligible concepts, the courts "look to whether the claims . . . focus on a specific means or method that improves the relevant technology or are instead directed to a result or effect that itself is the abstract idea and merely invoke generic processes and machinery." *McRO, Inc. v. Bandai Namco Games Am. Inc.*, 837 F.3d 1299, 1314 (Fed. Cir. 2016).

Merely applying an "abstract idea . . . on a generic computer" does not satisfy step one. *Bascom Glob. Internet Servs., Inc. v. AT&T Mobility LLC*, 827 F.3d 1341, 1348 (Fed. Cir. 2016). Nor does "[l]imiting the invention to a technological environment" such as the Internet transform an otherwise abstract idea into non-abstract one. *Berkheimer*, 881 F.3d at 1367. According to the Federal Circuit, a computer-based patent should specifically "describe how to solve the problem [it addresses] in a manner that encompasses something more than the principle in the abstract" to claim eligible subject matter at step one. *See Dropbox, Inc. v. Synchronoss Techs., Inc.*, 815 F. App'x 529, 533 (Fed. Cir. 2020) (Fed. Cir. 2020); *see also Ancora Techs., Inc. v. HTC Am., Inc.*, 908 F.3d 1343, 1348 (Fed. Cir. 2018) (holding an invention patentable at step one where the claim "specifically identifies how th[e] functional improvement is effectuated in an assertedly unexpected way"). Put another way, courts at Alice step one seek to determine whether a patent's claimed advance represents a concrete "technological solution to a technological problem." *See Packet Intel. LLC v. NetScout Sys., Inc.*, 965 F.3d 1299, 1309 (Fed. Cir. 2020); *see also Prism Techs. LLC v. T-Mobile USA, Inc.*, 696 F. App'x 1014, 1017 (Fed. Cir. 2017) (denying eligibility at step one because the claims did not "cover a concrete, specific solution to a real-world problem"). In this regard, the focus is placed on a patent's specificity.

If a patent is directed to an abstract idea at Alice step one, then Alice step two considers whether "the elements of [a] claim both individually and as an ordered combination" go beyond "well-understood, routine, [and] conventional activit[ies] previously known to the industry." *Alice*, 573 U.S. at 217, 225 (quoting *Mayo Collaborative Services*, 566 U.S. at 73, 79). This second step is also described as "a search for an inventive concept." *Id.* at 217–18 (quoting *Mayo Collaborative Services*, 566 U.S. at 72–73). In the case of a computer-implemented invention, the

Federal Circuit has held that components recited in the claims "must involve more than performance of 'well-understood, routine, conventional activit[ies]' previously known to the industry" to render an abstract idea patent-eligible. *In re TLI Commc'ns LLC Pat. Litig.*, 823 F.3d 607, 613 (Fed. Cir. 2016). The components themselves may supply an inventive concept if they amount to more than "generic computer components." *See Customedia Techs., LLC v. Dish Network Corp.*, 951 F.3d 1359, 1366 (Fed. Cir. 2020). Further, "an inventive concept can also be found in the non-conventional and non-generic arrangement of known, conventional pieces" of computing components. *Bascom*, 827 F.3d at 1350.

Courts have recognized that step one and step two of the Alice test may overlap in many "cases involving computer-related claims," such that "an analysis of whether there are arguably concrete improvements in the recited computer technology could take place" under both steps. *See Enfish, LLC v. Microsoft Corp.*, 822 F.3d 1327, 1339 (Fed. Cir. 2016); *see also Amdocs (Israel) Ltd. v. Openet Telecom, Inc.*, 841 F.3d 1288, 1294 (Fed. Cir. 2016) (observing that recent cases ''suggest that there is considerable overlap between step one and step two, and in some situations [the inventive concept] analysis could be accomplished without going beyond step one.''). Therefore, this Court previously adopted "a flexible approach in 'characteriz[ing] what the claims are directed to,' taking both step[]one and step[]two considerations into account[.]" *Fortinet, Inc. v. Forescout Techs., Inc.*, No. 20-CV-03343-EMC, 2021 WL 2412995, at *8 (N.D. Cal. June 14, 2021). In addition, this Court previously discussed the role of a patent's specification at length and concluded that "at this still-early stage of the litigation, [the Court should] construe the focus of [the patent] 'in light of the specification,' . . . and to credit the specification's account of whether and how 'the claimed invention achieves multiple technological improvements' over the prior art[.]" *Id.* at *10; *see also Enfish*, 822 F.3d at 1335.

1. The '489 Patent

The '489 Patent concerns a method and a system for providing security to a network by "identifying an unauthorized user who is attempting to gain access to a node on the network, and . . . actively blocking that unauthorized user from further activities." '489 Patent, at abstract. This is accomplished by marking false data which allows identification of intrusions of a network. *Id.*

Claim 1 states the following:

> 1. A method for detecting and handling a communication from an unauthorized source on a network, the method comprising the steps of:
>
> (a) receiving the communication from the unauthorized source,
>
> (b) analyzing the communication for detecting an information gathering procedure;
>
> (c) if said information-gathering procedure is detected, indicating a source address of the communication as a suspected network reconnaissance collector;
>
> (d) returning an earmark to said Suspected reconnaissance collector, Such that Said earmark includes specially crafted false data, and such that said earmark includes data that can serve to identify an unauthorized Source;
>
> (e) analyzing each subsequent communication for a presence of Said earmark,
>
> (f) if said earmark is present, indicating source address of the communication as a suspected network reconnaissance collector, and
>
> (g) if said source address is said intruder source address, applying intrusion handling procedures towards the communication from said intruder source address.

'489 Patent, at Claim 1.

a. Step One

Courts at Alice step one seek to determine whether a patent represents a concrete "technological solution to a technological problem." *Packet Intel.*, 965 F.3d at 1309. Fortinet argues that the '489 Patent is directed to the abstract idea of detecting unauthorized users by baiting them with false information, then waiting for that falsified data to appear to take action against them. Docket No. 115 ("Mot.") at 8. Fortinet argues that the idea of "baiting" an intruder with false information is a well-known "method of organizing human activity" that is impermissibly abstract under *Alice*. *Id.* Further, Fortinet notes that collecting and analyzing information for detecting and notifying fraud or misuse was already found to be abstract by the Federal Circuit. *Id.* (citing *Bozeman Fin. LLC v. Fed. Rsrv. Bank of Atlanta*, 955 F.3d 971, 977 (Fed. Cir. 2020); *FairWarning IP, LLC v. Iatric Sys., Inc.*, 839 F.3d 1089, 1094 (Fed. Cir. 2016)).

Therefore, Fortinet argues that the claim "do[es] no more than break the abstract idea into basic steps." Reply at 2 (quoting *Ultramercial, Inc. v. Hulu, LLC*, 772 F.3d 709, 714 (Fed. Cir. 2014). Further, Fortinet notes that what exactly constitutes "specially crafted" data is undescribed. *Id.*

Forescout counters that the '489 Patent claims a specific improvement over the prior art: improved accuracy. Docket No. 116 ("Opp'n") at 5. Forescout argues that this is a problem specific to computer networks and the '489 Patent recites a specific technique for computer network security that departs from earlier approaches. *Id.* at 6.

The Court first examines whether the '489 Patent addresses a technological problem. Fortinet argues that the presence of intruders is not confined to a computer network environment, therefore, the problem is not unique to computer networks. Mot. at 8. Forescout notes that conventional networks used heuristics, resulting in many false alarms that "nullifie[d] the usefulness of such systems[,]" which created "a need for a useful security protection method." Opp'n at 3–5. Therefore, Forescout contends that the '489 Patent claims an improvement directed toward solving a unique problem to intruder detection on computer networks, which is an "improvement in computer network technology." Opp'n at 5 (citing *SRI Int'l, Inc. v. Cisco Sys., Inc.*, 930 F.3d 1295, 1303 (Fed. Cir. 2019), *vacated in part on other grounds*, 930 F.3d 1295 (Fed. Cir. 2019)). As Fortinet states, baiting an intruder is an abstract idea, and the mere fact that the claim is limited to a network environment does not make it non-abstract. *Intell. Ventures I LLC v. Cap. One Bank (USA)*, 792 F.3d 1363, 1366 (Fed. Cir. 2015) ("An abstract idea does not become nonabstract by limiting the invention to a particular field of use or technological environment, such as the Internet."). However, while intruders are not confined to a computer network, "identifying hackers or potential intruders to the network" is a technological problem arising in computer networks. *SRI Int'l*, 930 F.3d at 1303.

Second, the parties argue as to whether the claimed improvement is a technological solution. Claim 1 can be summarized as follows: "receiving" communication from a device, "analyzing" it for suspicious activity, "identifying" the intruder using an earmark that is "specially crafted false data," "analyzing" subsequent communications for the presence of the earmark, then "applying" intruder handling protocols. Fortinet argues that the '489 Patent simply attempts to

claim the idea of "baiting an intruder with false information[,]"a "well-known human activity" that "constitute[s an] abstract idea" like *Ericsson*. Mot. a 9–10 (citing *Ericsson Inc. v. TCL Commc'n Tech. Holdings Ltd.*, 955 F.3d 1317, 1326–27 (Fed. Cir. 2020) (finding that claims were ineligible for being directed to the abstract idea of controlling access to resources).

However, unlike Fortinet's representation, the '489 Patent is distinguished from *Ericsson*, as the claimed method is not the type of activity that "can be performed in the human mind, or by a human using a pen and paper." *Id.* *Ericsson* does not apply because the human mind is not equipped to detect suspicious activity by using false data.

A closer analogy can be found in *SRI Int'l.* The patent in *SRI Int'l* claimed an automated computer network intrusion detection method "using a specific technique—using a plurality of network monitors that each analyze[d] specific types of data on the network and integrating reports from the monitors—to solve a technological problem arising in computer networks: identifying hackers or potential intruders into the network[.]" *SRI Int'l*, 930 F.3d at 1303. The Federal Circuit agreed with the district court that the claims were "more complex than merely reciting a known practice on the Internet and [were] better understood as being necessarily rooted in computer technology in order to solve a specific problem in the realm of computer networks." *Id.* The '489 Patent addresses the same specific technological problem of identifying potential intruders into the network and provides that while prior art would normally use a firewall to prevent unauthorized entry, the '489 Patent uses security modules with false information that allows the unauthorized source to be identified later. *Id.* at 4:48–50, 63–66. This technology-based approach can fairly be characterized as a technological solution directed to improving intruder detection on computer networks by improving accuracy, protecting the network, and avoiding false alarms. Opp'n at 5.

Fortinet argues that neither the language of the claims nor the specification detail technological specificity sufficient to demonstrate that the invention is a technological improvement. Reply at 2; Mot. a 9–10. Forescout counters that the '489 Patent's claims a specific technological solution in its use of "specially crafted false data" and "imitative (fake) network services to identify and isolate intruders." Opp'n at 5–6. The parties disagree on whether

this "specially crafted false data" has the requisite specificity. Fortinet argues that "precisely how to 'specially craft' this data is not claimed, and instead is left entirely to the implementor . . . Any data that is in some way 'specially crafted,' such that it can be used to identify the bad actor, will suffice." Reply at 2. Indeed, Claim 1 describes "specially crafted false data" sparsely as an "earmark includ[ing] data that can serve to identify an unauthorized source." '489 Patent, at Claim 1. Limited solely to the language of Claim 1, the '489 Patent should arguably be deemed abstract due to its lack of specificity.

However, the specification provides a greater degree of technological specificity that may satisfy the step one inquiry. According to the specification, the mark is "designed such that any attempt by an unauthorized user to use such false data results in the immediate identification of the unauthorized user as hostile." '489 Patent at 2:16–18. The mark also includes an identifier for later identifying the unauthorized user which "[p]referably . . . features numeric data, which can be identified easily and preferably uniquely in order to avoid mistaken identification of an authorized user as being unauthorized." *Id.* at 5:7–12. The specification also provides that this mark is attached after identifying possible unauthorized users that perform a "scan," which is a method of information collection used by unauthorized users. *Id.* at 6:10–11. Once a "scan" is detected, the unauthorized user is added to the intruder database, and a mark is returned to the user. *Id.* at 28–34. If the unauthorized user returns, the suspected user is matched with the previous source address stored in the intruder database, allowing additional confirmation that the suspect is actually hostile. *Id.* at 39–51. This mark database is preferably "structured such that each entry has the form of <IP Address, Port Number>. Such an entry represents a false network service, which does not exist on the network. Thus, accessing such a network service is considered to be hostile, indicating the presence of an intruder, as legitimate users would not attempt to access the service." *Id.* at 6:45–51. This detail regarding the "specially crafted false data" and "false network service" suggests that the '489 Patent describes a specific technique to solve a technological problem arising in computer networks. Further, the dependent claims describe the limitations in greater detail. For example, Claim 9 limits the information gathering procedure to be selected from the group consisting of a scan, a Domain Name Service (DNS) zone transfer, a

"finger" probe, NIS/LDAP interrogation, and sniffing. '489 Patent at Claim 9. The "specially crafted false data" used for Claim 9 are specifically defined in the specification as below:

> The DNS zone transfer probe involves the interrogation of a DNS server in order to receive a list of host names and addresses in the network. Marks against this method are prepared by defining names and addresses of non-existent hosts within the network at the DNS server. The identifier associated with such a mark is the IP address of the non existent host.
>
> The "finger probe is performed by interrogating a host computer, which is a node on the network, for active users with the "finger" service of the UNIX operating system. Replying to such an interrogation with the name of a non-existent user or users provides the marks for this method. The mark is in the form of <IP address, user name>, such that this combination provides the identifier for detecting any subsequent intrusion attempts.
>
> NIS/LDAP interrogation involves NIS and/or LDAP data bases which are often used to store site-specific information and which provide access methods over the network. Unless these databases are protected, the unauthorized user can interrogate these databases remotely, and retrieve information such as user names, encrypted passwords, network node (computer) names and addresses, and so forth. Marks against this probing method are prepared by constructing a fake NIS and/or LDAP database, which contain any of the previously described information items as mark.
>
> The sniffing method involves recording network activities within the network, particularly after the unauthorized user has penetrated the network and has gained high level privileges . . . Marks against this probing method are provided by simulating sessions over the network, and including fake user names and passwords during these "sessions". The mark has the form of <IP address, user name, password>.

Id. at 7:61–8:26.

Fortinet may ultimately prove that the above description of the "specially crafted false data" or "false network service" provides no meaningful detail sufficient to take the invention beyond an abstract concept. However, the Court cannot make such a determination on a Rule 12(b)(6) motion. For the purposes of a motion to dismiss, all factual inferences are made in favor of the patentholder. The Court cannot conclude as a matter of law at this juncture that the patent claims are directed to an abstract idea rather than a technological improvement in computer technology.

b. Step Two

Nevertheless, even if the Court were to find the '489 Patent to be ineligible subject matter at step one, the Court is reluctant to find the '489 Patent ineligible at step two because the same concerns recited at step one apply to step two. "An analysis of whether there are arguably concrete improvements in the recited computer technology could take place under either step one or step two." *Fortinet*, 2021 WL 2412995 at *8 (quoting *Enfish*, 822 F.3d at 1339).

At Alice step two, the Court must determine whether the claims contain an "inventive concept" sufficient to "transform" the abstract idea of using an earmark into a patent-eligible "application" of the abstract idea. *Alice*, 573 U.S. at 217–18. Alice step two is satisfied when the claims recite more than performance of "well-understood, routine, conventional activities[,]" which is a question of fact. *Id.* at 225; *Berkheimer*, 881 F.3d at 1368.

Fortinet argues that the '489 Patent fails to recite an inventive concept, as it simply instructs the practitioner to "implement the abstract idea . . . on a generic computer," which "does nothing significant to differentiate a process from ordinary mental processes," and therefore should be excluded under § 101. Mot. at 10 (quoting *Alice*, 573 U.S. at 225; *Elec. Power Grp., LLC v. Alstom S.A.*, 830 F.3d 1350, 1355 (Fed. Cir. 2016)). According to Fortinet, this method does not require any configuration other than the conventional machine on a conventional network and therefore does not "transform" the idea into an invention. *Id.*

Forescout argues that "an inventive concept can be found in the non-conventional and non-generic arrangement of known, conventional pieces." *Bascom*, 827 F.3d at 1349–50. Forescout argues that the claims "when considered as a whole, detect and mitigate any unauthorized, hostile sources by using false data requested by that source," which is an inventive concept. Opp'n at 7. Therefore, Forescout states that it is premature to conclude that the components of the claims as combined were "well-understood, routine, and conventional" at the time of the invention in 1999. *Id.*

Like step one, it would be difficult to conclude at this point that the ordered combination of elements lacks an inventive concept. The '489 Patent, on its face, plausibly presents claims directed to specific improvements that recite more than what was conventional. Forescout notes

that conventional systems used heuristics which had a "high rate of false alarms, which nullifie[d]" the usefulness of such systems. Opp'n at 7. Further, the specification states that the invention departs from the prior art method, which featured a firewall installed at the entry point to prevent unauthorized entry that could be circumvented. '489 Patent at 4:42–47. The current invention places security modules containing the earmark instead of a firewall and identifies an unauthorized source as hostile "by analyzing its communication for false earmarked data" and providing "an imitative, false network service rather than . . . the actual service on the network." '489 Patent at 7:27–28. Forescout contends that this combination results in much more accurate hostile source identifications and allows confirmation, which are improvements over the conventional systems. Opp'n at 7. (citing '489 Patent at 1:36–37). Like step one, it cannot be determined at this stage of the litigation whether this "false earmarked data," "false network service," or their combination thereof were "well-understood, routine, and conventional to a skilled artisan in the relevant field"; questions of fact "must be proven by clear and convincing evidence." *See Berkheimer*, 881 F.3d at 1360. Therefore, the Court denies the motion to dismiss for the '498 Patent.

2. The '116 Patent

The '116 Patent concerns "device classification." Specifically, "systems, methods, and related technologies for device classification are described. Claim 1 recites:

> 1. A method comprising:
>
> Detecting a device coupled to a network in response to the device being coupled to the network;
>
> Accessing first data associated with the device from an agent installed on the device;
>
> Accessing second data associated with the device from an external system, wherein the second data associated with the device comprises traffic data associated with the device;
>
> Analyzing the traffic data of the device;
>
> Determining a classification for the device based on the first data associated with the device and the traffic data;
>
> and storing the classification for the device.

'116 Patent, at Claim 1.

a. Step One

At Alice step one, Fortinet argues that the '116 Patent's claims are directed to an abstract idea of classifying devices on a network using more than one source of data. Mot. at 14. Fortinet further argues that the claims describe the "data" being analyzed only in "extremely generic terms," which could be any data about the device. *Id.* Fortinet relies on several Federal Circuit cases that had found claims combining multiple sources of data to be abstract. *Id.* (citing *Credit Acceptance Corp. v. Westlake Servs.*, 859 F.3d 1044, 1054 (Fed. Cir. 2017) (finding claims reciting a method of "combining [] two sources of information to create a financing package" to be directed to an abstract idea); *Bozeman*, 955 F.3d at 979 (finding claims reciting a method of "reducing check fraud by receiving financial transaction data from two sources" to be directed to an abstract idea)). Fortinet also notes that the Federal Circuit has found the idea of classifying devices to be a well-known "method of organizing a human activity." *Id.* (citing *Content Extraction & Transmission LLC v. Wells Fargo Bank, Nat. Ass'n*, 776 F.3d 1343, 1347 (Fed. Cir. 2014) (finding claims reciting a method of processing information and storing them according to their classification to be abstract)).

The '116 Patent seems to claim a solution to a problem unique to computer networks that improves network monitoring. The '116 Patent states that previous conventions resulted in frequent false negatives and false positives which could "only provide high-level rough classifications" that were unusable. Opp'n at 9 (citing '116 Patent at 2:51–54). This problem was exacerbated by the proliferation of the Internet of Things ("IoT"), which are "systems and devices being used for various applications and locations ranging from households to large industrial environments." *Id.* This problem of inaccuracy that is exacerbated by the IoT recites a problem unique to computer networks and is improved by the '116 Patent.

The next question is then whether the claims "specifically identifies how th[e] functional improvement is effectuated in an assuredly unexpected way." *Ancora Techs.*, 908 F.3d at 1348. Forescout argues that this problem of inaccuracy is solved by "combining multiple sources: an agent installed on the device and an external system" which contains "traffic data associated from

devices." Opp'n at 9–10; *see* '116 Patent 2:66–3:01, 9:56–57.

At first glance, the claimed method boils down to using two different sets of data to classify a device instead of using one set of data. Merely using several sources of information does not make an abstract idea any less abstract; nor does merely applying an "abstract idea . . . on a generic computer" satisfy step one. *Bascom*, 827 F.3d at 1348. Collecting and analyzing data is an abstract concept. *See, e.g.*, *Electric Power Group, LLC*, 830 F.3d at 1351–56 (holding that "systems and methods for performing real-time performance monitoring . . . by collecting data from multiple data sources, analyzing the data, and displaying the results" was abstract because the claims focused merely on the abstract idea of collecting, analyzing, and displaying information).

However, the '116 Patent contains greater technological specificity than cases relied on by Fortinet. *Bozeman* was directed to the abstract idea of collecting information to check for transaction fraud or errors. 955 F.3d at 980. *Credit Acceptance* was directed to the abstract idea of processing an application for financing a purchase. 859 F.3d at 1054. Unlike these cases, the '116 Patent is directed to an improvement in computer network security. Opp'n at 11.

A better analogy can be found in *SRI Int'l*, in which the Federal Circuit found that a method of hierarchical event monitoring and analysis within a network that "deploy[ed] a plurality of network monitors, detect[ed] suspicious network activity based on analysis of network traffic data selected from one or more of [the listed categories], generat[ed] . . . reports . . . and automatically receiv[ed] and integrat[ed] the reports of suspicious activity, by one or more hierarchical monitors" to be sufficiently specific. *SRI Int'l*, 930 F.3d at 1303 ("The claims are directed to using a specific technique—using a plurality of network monitors that each analyze specific types of data on the network and integrating reports from the monitors."). The Federal Circuit noted that "the claims are not directed to just analyzing data from multiple sources . . . [but] to an improvement in computer network technology" because the claims "recited using network monitors to detect suspicious network activity based on analysis of network traffic data, generating reports of that suspicious activity, and integrating those reports using hierarchical monitors." *Id.*

Taking the language of the claims and the specification together, the '116 Patent provides greater technological specificity than *Credit Acceptance*, *Bozeman*, and *Electric Power Group* and more closely mirrors *SRI Int'l*. Claim 1 clarifies that the second set of data used is from "an external system" and "comprises traffic data" associated with the device. '116 Patent at Claim 1. The specification further provides that the analysis of this traffic data can be through "active" or "passive" traffic analysis, which may be a configurable option by the user on a per device basis or network segment basis. *Id.* at 6:33–47. Passive traffic analysis includes observing "communications to and from the device to be classified with other devices." *Id.* at 6:37–39. Active traffic analysis may analyze behavior "in response to communication that is sent to the device to be classified from the device performing classification" by methods such as actively probing ports. *Id.* at 6:35, 40–44. This suggests that characterizing the '116 Patent as merely combining two sets of data may be an oversimplification, as the specification indicates that the usage of traffic data enables the device to not only receive data but actively seek it out by sending communications to the device and observing its response. *See id.* The specification further suggests that it is possible to use passive traffic analysis to determine classification and use active traffic analysis to "confirm or fine tune the classification." *Id.* at 6:49–52. Therefore, the two types of analysis enabled by traffic data may also allow an additional confirmation step. *See id.* This level of computer network-specific detail provided in the specification suggests that the patent may be "understood as being necessarily rooted in computer technology in order to solve a specific problem in the realm of computer networks." *See SRI Int'l*, 930 F.3d at 1303. Therefore, the Court declines to find the '116 Patent abstract at Alice step one on a Rule 12(b)(6) motion.

b. Step Two

The Court does not need to consider Alice step two, as it does not find the '116 Patent directed to an abstract ineligible subject matter at step one. Nevertheless, the Court also declines to find that the '116 Patent fail Alice step two at this stage. Step two of Alice requires an "inventive concept" that must involve more than "well-understood, routine, conventional activity previously known to the industry." *Id.* at 225. Any abstract idea must be "transform[ed]" into a patent-eligible "application" of the abstract idea to pass this test. *Alice*, 573 U.S. at 217–18.

Fortinet argues that the '116 Patent fails to recite an inventive concept because claim 1 recites simple components "recited at a high level of generality[,]" and the steps of "accessing" and "analyzing" data and "determining" classification simply recites the abstract idea itself. Fortinet claims that the configuration provided does not add sufficient substance to the underlying abstract idea and merely serves as "a conduit for the abstract idea." *Id.* Therefore, nothing transforms the idea into an invention and merely uses "well-understood, routine, conventional components to apply [an] abstract idea." Mot. at 16 (citing *Yu v. Apple, Inc.*, 1 F.4th 1040, 1045 (Fed. Cir. 2021). Fortinet analogizes the '116 Patent to the patent in *Universal Secure Registry*, in which the court found that the claims failed to recite a new authentication technique since the techniques being combined were known, and their combination failed to "achieve[] more than the expected sum of the security provided by each technique." Reply at 7 (citing *Universal Secure Registry LLC v. Apple Inc.*, No. 2020-2044, 2021 WL 3778395, at *10 (Fed. Cir. Aug. 26, 2021).

Forescout contends that the claims considered as a whole transform the abstract idea into a "particular, practical application of that abstract idea[.]" Opp'n at 12 (citing *Bascom*, 827 F.3d at 1349–50). Forescout argues that having a second data set composed of traffic data solves the unique problem of inaccurate and unreliable classifications in conventional network monitoring in a specific and technological way beyond the general and expected improvement of accuracy achieved through using additional datasets. *Id.*

Here, the Court finds similarity to *Amdocs*, a case with a similar patent claim that combined two different datasets. *Amdocs*, 841 F.3d at 1300. In *Amdocs*, the Federal Circuit found that claims correlating two network accounting records to enhance the first record had an inventive concept, providing unconventional solutions to technological problems and advantages over the prior art. *Id.* The Federal Circuit examined previous decisions that discussed claims related to the collection and classification of data and explained that "claims involving the mere collection and manipulation of information"—like *Content Extraction* and *In re TLI Commc'ns*— "do not satisfy § 101—under either step one or step two." *Id.* at 1300; *Content Extraction*, 776 F.3d at 1347 (finding that collecting data, recognizing certain data within the collected data set, and storing the recognized data was abstract); *In re TLI Commc'ns*, 823 F.3d at 613 (finding that the claims were

directed to the abstract idea of "classifying and storing digital images in an organized manner."). On the other hand, eligibility can be found "when somewhat facially-similar claims are directed to an improvement in computer functionality under step one, *see Enfish*, 822 F.3d at 1335, or recite a sufficiently inventive concept under step two—particularly when the claims solve a technology-based problem, even with conventional, general components, combined in an unconventional manner." *Id.* (citing *Bascom*, 827 F.3d at 1349–52; *DDR Holdings, LLC v. Hotels.com, L.P.*, 773 F.3d 1245, 1256–59 (Fed. Cir. 2014) (finding that the "ordered combination" of the elements recited an invention that was not merely routine or conventional).

The Federal Circuit then concluded that the claims were "much closer to those in *Bascom* and *DDR Holdings* than those in . . . *Content Extraction* and *In re TLI Commc'ns*." *Id.* at 1300–02 (noting that in *Bascom*, the individual limitations were generic, but the ordered combination of them recited an inventive concept that improved the performance of the computer system itself because installing a filtering tool at a specific location permitted both the benefits of a filter on a local computer and an internet server). The solution only required "generic components," including network devices and "gatherers" which "gather" information. *Id.* However, like *Bascom*, the benefits of the patent were possible because of the distributed, remote enhancement that produced an unconventional result of reduced data flows and the possibility of a smaller database. "Enhance," which was construed as meaning "to apply a number of field enhancements in a distributed fashion[,]" was a "critical advancement over the prior art" by enabling "load distribution." *Id.* at 1300–02. This "enhancing limitation" which depended on the invention's "distributed architecture" and the "network devices and gatherers . . . working together in a distributed manner" "necessarily required that these generic components operate in an unconventional manner to achieve an improvement in computer functionality." *Id.* at 1301–02.

Similarly, Forescout plausibly asserts that the combination of the elements recites an invention beyond what was merely routine or conventional that "improved the performance of the computer system itself," through its use of "traffic data" and "external system." The '116 Patent describes the conventional classification methodologies that relied on media access control (MAC) addresses and hypertext transfer protocol (HTTP) user-agent strings as "particularly limited and

narrow in their classification abilities and in many cases unable to classify devices." '116 Patent at 1:18–23. This is because "certain characteristics of a particular device (e.g., whether such a device is an access point) can be more difficult to determine with a high degree of accuracy." *Id.* at 2:8–17. According to Forescout, this technological problem is solved by the combination of two datasets, wherein the second set of data is retrieved from an external system and comprised of traffic data. *Id.* As discussed in the Alice step one analysis, the specification of the '116 Patent suggests that the usage of traffic information may not merely act as additional collected data but be specifically used to "confirm or fine tune the classification" through its two types of analysis. '116 Patent at 6:49–52. Further, the usage of an "external system" and "traffic data" may provide not only an additional confirmation process but also a more comprehensible view of the device. *See* '116 Patent at 10:16–21, 6:49–52. An example data flow of device information provided in the specification indicates that "the traffic and log analysis component may provide comprehensive layer 2-layer 7 device information as well as device authentication information (e.g., device login information) and segmentation information (e.g., network segment[s] such as a data center or accounting network address range)." *Id.* at 10: 17–21.

Taking the specification into account, the '116 Patent seems closer to the claims in *Amdocs* than the claims in *Universal Secure Registry*. Unlike *Universal Secure Registry*, in which nothing in the specification or motion indicated that the claim achieves more than the "expected sum" of the two datasets, the claims here suggest results beyond the expected sum. While Fortinet argues that the features of the claim are merely "conventional" and do not amount to a meaningful and unexpected result, the Court cannot make this assumption. Inferences must be resolved in Forescout's favor at the motion to dismiss stage, and there is a plausible argument that the above features constitute an inventive concept. *Berkeimer*, 881 F.3d at 1368. Like *Amdocs*, the use of a second data from an "external system" comprising of "traffic data" which includes more than, e.g., mere summarizing of data, may "operate in an unconventional manner to achieve an improvement in computer functionality." *Id.* at 1300–01. Absent further developments in this case such as claim construction or expert testimony, the Court cannot conclude at this juncture whether there is an "inventive concept" that goes beyond that which is "well-understood, routine and conventional

to a skilled artisan in the relevant field." *Berkheimer*, 881 F.3d at 1368.

3. The '278 Patent

The '278 Patent relates to a method of compliance monitoring in which the claim "detect[s]" a device, "determine[s] a classification of the device[,]" "accesse[s] a compliance rule[,]" "perform[s]" a compliance scan, then performs an "action" based on its compliance level. '278 Patent at Claim 1. Claim 1 recites:

> 1. A method comprising
>
> detecting, by a compliance monitoring device, a device coupled to a network in response to the device being coupled to the network;
>
> determining a classification of the device based on traffic information associated with the device;
>
> accessing a compliance rule based on the classification of the device, wherein the compliance rule is a standard based compliance rule;
>
> performing, by a processing device of the compliance monitoring device, a compliance scan on the device based on the compliance rule;
>
> determining a compliance level of the device based on a result of the compliance scan of the device; and performing an action based on the compliance level.

Id.

a. Step One

Fortinet argues that the '278 Patent is directed to the abstract idea of assessing compliance based on device classification. Mot. at 20 (citing *In re TLI Commc'ns*, 823 F.3d at 611). It argues that the idea of treating devices differently for compliance purposes is a common method of organizing human activity and often a necessary step in assessing compliance with any set of regulations. *Id.* It also argues that the compliance scanning uses existing technology and merely "reduce[s] the burden on a system administrator by automating a task they would already perform manually in effectively the same way." Reply at 11.

Forescout counters that the '278 Patent allows for "automated and continuous compliance checks," which solves a problem specific to computer networks using a specific technological solution: allowing automated use of different compliance rules for different types of devices rather

than manually doing so. *Id.* at 15, 18. Forescout compares the '278 Patent to the patent in *Finjan*, asserting that it has similar improvements that "enables more flexible and nuanced" compliance monitoring and that the classification allows customization of the compliance scans. Opp'n at 16 (citing *Finjan, Inc. v. Blue Coat Sys.*, 879 F.3d 1299, 1299 (Fed. Cir. 2018).

First, the '278 Patent seems to identify a technological problem arising in computer networks: preventing "access to network resources by unauthorized devices" and "effectively manag[ing] access" for authorized devices. This problem is unique to computer networks in the face of the "proliferation of network-connected devices" such as smartphones, tablets and wearable devices. '278 Patent at 1:50–55.

However, Forescout's argument that this technological problem is solved using a technological solution is not persuasive. It describes the solution only as follows: "e.g., the standard based compliance rule, automatic classification, and automatic compliance scanning" which "improves the functioning of the computer network . . . by preventing unauthorized access by non-compliant devices." Opp'n at 16. As such, Forescout fails to "specifically identif[y] how th[e] functional improvement is effectuated in an assuredly unexpected way." *Ancora Techs.*, 908 F.3d at 1348. The '278 Patent essentially boils down to assessing compliance based on a device classification, treating devices differently for compliance purposes, and automating the implementation by a computer. *See* Mot. at 19.

As Fortinet contends, classification of data is a well-established "basic concept" under Alice step one, and merely combining the idea of classifying and applying a compliance action based on the classification does not make the patent non-abstract. *RecogniCorp, LLC v. Nintendo Co.*, 855 F.3d 1322, 1327 (Fed. Cir. 2017) ("Adding one abstract idea . . . to another abstract idea . . . does not render the claim non-abstract."). The limitations of the claims are also generic. First, the method detects a device using any "compliance monitoring device," but this device can be a "computing system, [or] a network device . . . etc." that monitors for compliance—i.e., generic computer and network components which amounts to merely "a generic environment in which to carry out the abstract idea." '278 Patent at 4:14–19; *In re TLI Commc'ns*, 823 F.3d at 611. The classification of the device is based on "traffic information," but the significance of this traffic

information is not specified in the patent nor argued by Forescout. The "standard based compliance rule" is no less generic, as the specification describes this limitation as "using available standard based compliance content[,]" meaning that any available compliance rule falls under Claim 1. '278 Patent at 3:21. Once a compliance scan is performed based on the rule, then an "action" is performed. Again, this action can be anything. Forescout attempts to argue that this "action" limitation is narrowed in its dependent claims, which "provide exemplary actions, including 'changing network access,' 'automatically initiating an update service,' and 'initiating a patch service.'" Opp'n at 16. However, these dependent claims do not contain meaningful limitations as they provide no more than generic compliance actions. Therefore, the claim describes a combination of abstract ideas using generic parts and processes, which generally boils down to performing a classification and treating the classified items differently depending on their classes—an abstract idea.

Similarly, the need to perform tasks automatically by itself is not a unique technical problem. *In re TLI Commc'ns*, 823 F.3d at 613; *OIP Techs., Inc. v. Amazon.com, Inc.*, 788 F.3d 1359, 1363 (Fed. Cir. 2015); *Cellspin Soft, Inc. v. Fitbit, Inc.*, 927 F.3d 1306, 1316 (Fed. Cir. 2019). Making a "process more efficient" in itself does not "render an abstract idea less abstract." *Secured Mail Sols. LLC v. Universal Wilde, Inc.*, 873 F.3d 905, 910 (Fed. Cir. 2017). Therefore, mere automation of manual processes using generic computers as a tool does not constitute a patentable improvement in computer technology. *Credit Acceptance*, 859 F.3d at 1055.

Finally, Forescout's analogy to Finjan that the '278 Patent similarly "enables more flexible and nuanced network compliance management" is inapposite because Forescout ignores the larger ground on which the Federal Circuit found the claim non-abstract. Opp'n at 16; *Finjan*, 879 F.3d at 1304. In *Finjan*, the Federal Circuit found a patent that described a new "behavior-based" approach to virus scanning in contrast to the traditional "code-matching" system to be eligible. 879 F.3d at 1304. However, Forescout does not claim a new approach to compliance management. Forescout fails to demonstrate a new approach here comparable to that in *Finjan*. *See* Opp'n at 18.

For the foregoing reasons, the Court finds the '278 Patent directed to the abstract idea of

automatically classifying devices and then assessing compliance and performing actions based on compliance rules.

b. Step Two

Accepting that the asserted claims are directed to an abstract idea, the Court turns to step two to assess whether "the elements of each claim both individually and 'as an ordered combination' . . . 'transform the nature of the claim' into a patent-eligible application." *Alice*, 573 U.S. at 218.

Fortinet argues that the '278 Patent fails to recite an inventive concept and merely recites the abstract idea of assessing compliance based on device classification. Mot. at 20. Fortinet argues that the compliance monitoring device merely detects and scans devices, creating "a generic environment"—i.e., a computer network—" in which to carry out the abstract idea." *Id.* (citing *Ericsson*, 955 F.3d at 1326–27). Fortinet further notes that only general and conventional hardware components are mentioned in the '278 Patent. Reply at 12 (citing '278 Patent at 2:10–15). Forescout alleges that "the claims, when considered as a whole, perform a specific sequence of device classification and standard based compliance scanning that was not well-understood, routine, or conventional at the time of the invention." Opp'n at 18–20.

From the specification it is clear, and Forescout does not argue otherwise, that the claims' individual limitations recite only generic computer and network components. However, an inventive concept can be found in the "non-conventional and non-generic arrangement of known, conventional pieces." *Bascom*, 827 F.3d at 1350; *see also DDR Holdings*, 773 F.3d at 1256–59; *Amdocs*, 841 F.3d at 1300–01.

According to Forescout and the '278 Patent, the prior art used a "golden image"—"a computing system image that has been customized to a particular configuration that may be copied onto multiple computing systems or devices." '278 Patent at 2:2–5; Opp'n at 14–15. Forescout argues that the manual and pre-specified "golden image" approach is improved by the use of "adaptable, device-specific compliance standards" achieved through "combin[ing] standards based compliance with policy based network access control [("NAC")]." Opp'n at 17, 20 (citing '278 Patent at 2:25–28).

The '278 Patent states that its novel combination "allows the direct linking of compliance within a NAC product to the results of a compliance scan based on the content." '278 Patent at 3:26–28. Notably, the specification points out that the combination is advantageous because "the use of standards based compliance content . . . is not dependent on or related to the particular [NAC] solution being used." *Id.* at 3:33–37. The specification further explains that "the modular nature of [the] system may allow the components to be independent and allow flexibility to enable or disable individual components or to extent/upgrade components without affecting other components thereby providing scalability and extensibility." *Id.* at 8:30–35. Further, the use of standards based compliance content is defined technically rather than a "prose-based configuration checklist being input to a NAC based policy engine[,]" thereby "avoid[ing] misinterpretations or misconfigurations." *Id.* at 3:37–39.

Forescout also contends that "automated and multi-device compliance scanning" is a specific improvement over conventional systems. Opp'n at 19. The specification provides that "[a]utomated device compliance can be difficult to determine and review with existing methodologies." *Id.* at 2:6–10. According to Forescout, conventional systems had a problem—there being too many devices connected to a network at once—that a conventional classification system could not effectively manage. Opp'n at 19–20. Therefore, it claims that solving the computer-specific problem of enforcing compliance by the numerous and different types of devices on a network by automatically classifying them and applying a compliance rule is inventive and not merely conventional. *Id.* Device classification also allows for customizing the compliance scans such as performing a particular scan based on the device's operating system. Opp'n at 16–17 (citing '278 patent at 3:43–51 ("[T]he compliance scans can be performed on selected devices communicatively coupled to a network that have been classified as having a particular operating system, e.g., Microsoft Windows.")). The invention therefore "remove[s] the need for network administrators to have to manually specific [sic] IP addresses or IP address ranges for compliance scanning[,]" distinguishing the prior art approach of merely copying a "golden image," which is a previously specified "particular configuration." '278 Patent at 2:2–5; 3:43–51.

In addition, the '278 Patent suggests benefits beyond mere automation. As described previously, the invention allows for "adaptable and device-specific" compliance checks and its modular structure enables flexible control that provides "scalability and extensibility" and "avoid[s] misinterpretations or misconfigurations." Opp'n at 17; '278 Patent at 3:37–39; 8:30–35. It also "enables more flexible and nuanced" network compliance management through allowing customization rather than being limited to particular configurations like the conventional system. Opp'n at 16; '278 Patent at 5:29–34 ("For example, a user could open a compliance rules file and remove one or more rules or modify one or more weights associated with the rules."). Finally, the "automated and continuous compliance checks" "enable the ongoing monitoring of network devices and activity" and "can be also performed real-time[.]" *Id.* at 1:57–58; 3:5–7, 16–17.

Therefore, Forescout's claims at the very least plausibly recite an inventive concept under Alice step two, raising fact issues as to whether "conventional systems had difficulty effectively managing access to network resources and required manual compliance" that the '278 Patent "solved . . . by combining standards based compliance with policy based network access control[,]" enabling automation, multi-device compliance scanning, and customization. Opp'n at 20. Considering that "whether a claim element or combination of elements is well-understood, routine and conventional to a skilled artisan in the relevant field is a question of fact," and the court must weigh all factual inferences drawn from the specification in favor of Forescout, it is premature to decide eligibility at this stage of the litigation. *Berkheimer*, 881 F.3d at 1368. Further, Fortinet fails to establish that, as a matter of law, the ordered combination of the limitations in the claims is conventional and not innovative. Thus, the '278 Patent creates fact issues that preclude judgment for dismissal under Rule 12(b)(6), and the Court denies the motion to dismiss as to the '278 Patent.

4. The '764 Patent

The '764 Patent relates to a post-connection client certificate authentication. Claim 1 recites:

> 1. A system comprising:

> A memory; and
>
> A processing device operatively coupled to the memory, the processing device to:
>
> Detect a connection of an endpoint device at a network switch coupled to a network;
>
> Restrict access of the endpoint device to prevent the endpoint device from accessing resources of the network by applying a VLAN assignment to the network switch;
>
> Establish a connection with the endpoint device;
>
> Validate a client certificate corresponding to the endpoint device to authenticate the endpoint device as a corporate device, wherein to validate the client certificate, the processing device to:
>
> > Receive the client certificate from the endpoint name, the client certificate from the endpoint device, the client certificate comprising a subject name, a client public key and a digital signature of the client public key by a certificate authority;
> >
> > Retrieve a certificate authority certificate from the certificate authority, the certificate authority certificate comprising a certificate public key;
> >
> > Verify the digital signature of the client public key using the certificate authority public key; and
> >
> > Verify the subject name using the client public key; and
>
> Grant the endpoint device access to the resources of the network

'764 Patent, at Claim 1.

a. Step One

Fortinet argues that the '764 Patent is "directed to the abstract idea of validating authorization after connection" and that it uses generic computer components that perform their usual functions. Mot. at 24. Forescout again rebuts that the '764 Patent is not directed to an abstract idea but recites a "technological solution to a technological problem." According to Forescout, prior NAC devices had to choose between prior art solutions that offered either tight security or timeliness in granting access, but not both. Opp'n at 21. Further, it argues that prior art had a "major drawback" because of its "fail-closed" system. *Id.* For example, if the device fails in any way—i.e., a power outage—then all new connections were automatically denied,

which dampened user experience. *Id.* at 22. Forescout contends that the '764 Patent solves this problem in dependent Claim 5, which describes a "fail-open" system that grants access upon a NAC's failure during authentication. Therefore, the '764 Patent claims a functional improvement by allowing connection to the network with limited access, after which the device is validated, allowing for smoother user experience while blocking access to sensitive resources until verification. *Id.* at 22–25.

First, the balancing problem between user experience and network security is "a problem specifically arising in the realm of computer networks." *DDR Holdings*, 773 F.3d at 1257. The balance of speed and security required in network access is the type of issue that is unique to computer networks, especially considering the fact that improving either one necessarily compromises the other. There is thus a technological problem addressed by the '764.

The parties disagree as to whether Claim 1 is directed to a "specific technique." Opp'n at 23. Fortinet compares the '764 Patent to *Ericsson* and *Dropbox*. Mot. at 24–25; *Ericsson*, 955 F.3d at 1326–27 (finding that all four components of the claim "collapsed" into the abstract idea of controlling access to resources); *Dropbox*, 815 F. App'x at 529 (affirming the district court's finding that the patents were directed to functional results, not technological solutions). Although the '764 does not detail its technical aspects at length, it offers more technology-based improvements than *Dropbox* and *Ericsson*. In *Ericsson*, the patent's purported inventive concept did not appear in the language of the claims. *Ericsson*, 955 F.3d at 1328–9. In *Dropbox*, the claims "recited conventional elements in a purely functional manner, without implementation detail even in the specification." *Dropbox*, 815 F. App'x at 533.

In contrast, Claim 1 places emphasis on the new ordering of authentication using the specific technique of "post-connect certificate authentication," which enables "limited access" to a network instead of granting either complete access or no access at all. *See* '764 Patent at Claim 1; Opp'n at 24–25. The specification clarifies this technique as utilizing a "Public-Private Key Infrastructure with X.509 client certificates installed on connecting corporate endpoints" as "an alternative to the pre-connect 802.1x protocol, using a post-connect paradigm." '764 Patent at 2:22–26.

Claim 1 further provides that a processing device detects a connection of an endpoint device at a "network switch," "restricts access" by applying a "VLAN assignment" to the network switch, establishes a connection with the device, and authenticates the device by validating and verifying a client certificate provided by the device using a client "public key." *Id.* at Claim 1. If the client certificate is validated, the NAC device grants network access except for the most sensitive parts of the network. *Id.* at 2:44–49. Further evaluation is then possible to remove such restrictions or revoke the certificate. *Id.* at 2:49–56. According to the specification, this limited access is possible because a network switch may be "configured such that when it detects a new connection to the communication network, it immediately applies an access control list (ACL) or wireless role to prevent the connecting device accessing the connecting device accessing any network resources except for the NAC device and potentially other resources[.]" *Id.* at 2:26–34. An ACL manager can create, manage, and apply the ACL to switch to control what network resources a particular device has access to. *Id.* at 4:50–64. This level of detail contained in Claim 1 and the specification suggests that the '764 Patent does not simply describe a post-verification scenario but a solution that is technology-based.

Additionally, Claim 1 affords a completely new "fail-open" system described in Claim 5, which solves the problem of the "fail-close" system. Opp'n at 26. Claim 5 describes a system wherein the device is processed to "not restrict access of the endpoint device to the resources of the network when a NAC in the network suffers a failure during authentication of the endpoint device." '764 Patent at Claim 5. In a "fail-open" configuration, all ports on the switch are initially configured in an "open" mode instead of a "restrict" mode and only restricted when a new device is connected. '764 Patent at 5:10–17. Therefore, upon failure, during which the device is unable to restrict the ports, "all new and pending connections are granted access to the network as a matter of policy." *See id.* at 2:65–68; 5:14–17. This "fail-open" system is an improvement that "solv[es] yet another problem in the prior art related to failures (e.g., power failures) during authentication," and is possible through this novel post-connect paradigm of Claim 1. Opp'n at 23–25 (citing '764 Patent at 2:22–49, 57–3:3) ("Allowing a device to connect first and then performing certificate authentication before providing access to sensitive resources . . . allows for

a "fail-open" system[.]").

For the aforementioned reasons, the '764 Patent is "directed to improvements to the functionality of a computer or network platform itself," rather than simply "a process or system that qualifies an abstract idea for which computers are invoked merely as a tool." *Uniloc USA, Inc. v. LG Electronics USA, Inc.*, 957 F. 3d 1303, 1306–07 (Fed. Cir. 2020). Further, statements such that the '764 patent claims an improvement over the prior art approach of using the "802.1x protocol which ensures connecting devices are authenticated using an X.509 digital certificate, or other credentials, prior to even gaining access to the network[,]" must be taken as true in conducting the step-one inquiry. '764 Patent at 2:7–10; *see CardioNet*, 955 F.3d at 1369–70. Thus, the '764 Patent is not directed to a patent-ineligible abstract idea.

b. Step Two

As the '764 Patent is not directed to a patent-ineligible abstract idea, the inventive concept portion of the analysis need not be addressed. Nevertheless, even if the Court were to find the '764 Patent to be directed to an abstract idea, Forescout's allegations support a reasonable inference that the '764 Patent contains features that go beyond "well-understood, routine, and conventional" activities as described above. Alice step two "consider[s] the elements of each claim both individually and 'as an ordered combination' to determine whether the additional elements 'transform the nature of the claim' into a patent-eligible application." *Alice*, 573 U.S. at 217 (quoting *Mayo*, 566 U.S. at 77–78). Even if each element of Claim 1 individually is conventional, "an inventive concept can be found in the non-conventional and non-generic arrangement of known, conventional pieces." *Bascom*, 827 F.3d at 1350. Here, Forescout places the inventive concept on the new ordering of authentication, and this new ordering seems to be achieved through techniques that are arguably non-conventional and non-generic, to give "limited access" to a device. Opp'n at 25. This "post-connect paradigm" is purported to be an invention that is achieved using "a working Public-Private Key Infrastructure with X.509 client certificates" as "an alternative to the pre-connect 802.x protocol." *Id.*; 2:15–17, 2:23–26, 4:63–64. In addition, there are sufficient details in the specification to suggest that this novel approach achieves a specific improvement beyond the conventional system, as discussed in step one. *Enfish*, 822 F.3d

at 1339 ("[A]n analysis of whether there are concrete improvements in the recited computer technology could take place under step two.").

In sum, Forescout claims to improve conventional systems that "are limited and narrow in their authentication abilities[,] . . . negatively affect the user experience[,]" and compromise security. *Id.* at 27 (citing '764 patent at 1:17–20, 1:66–2:5). The achievement of the "post-connect paradigm" using "Public-Private Key Infrastructure with X.509 client certificates" was more than a "well-understood, routine, and conventional" technique. Therefore, the Court finds that the '764 Patent recites patent-eligible subject matter at both step one and step two of *Alice*.

B. Tortious Interference with Business Relations

Forescout alleges that Fortinet made false statements to Forescout's existing and prospective customers by "republish[ing]" its patent infringement complaint allegations to the media, and representing that they were facing "uncertain ground financially" to its customers. Mot. at 29. Fortinet claims that the tortious interference claim should be dismissed for three reasons: (1) the alleged conduct is not subject to this Court's subject matter jurisdiction, (2) the alleged statements are protected by federal law, which preempts the state law claim, and (3) the alleged conduct does not satisfy California law to state a claim for tortious interference. *Id.*

1. Subject Matter Jurisdiction

Under 28 U.S.C. § 1367(a), a federal district court which possesses original jurisdiction may hear other state law claims "that are so related to claims in the action within such original jurisdiction that they form part of the same case or controversy under Article III of the United States Constitution." In order for a claim to "form part of the same case or controversy," the claims must "derive from a common nucleus of operative fact." *United Mine Workers of Am. v. Gibbs*, 383 U.S. 715, 725 (1966).

28 U.S.C. § 1338(a) grants federal district courts original jurisdiction of any civil action arising under any federal statute relating to patents. *Christianson v. Colt Indus. Operating Corp.*, 486 U.S. 800, 800 (1988). In *Christianson*, the U.S. Supreme Court clarified the scope of § 1338(a), finding that § 1338(a) confers jurisdiction over not only causes of action created by federal patent law but also extends to cases in which the plaintiff's cause of action depends on the

resolution of a substantial question of federal patent law. *Additive Controls & Measurement Sys., Inc. v. Flowdata, Inc.*, 986 F.2d 476, 477–78 (Fed. Cir. 1993) (citing *Christianson,* 486 U.S. at 808–09).

Fortinet argues that there is no common nucleus of operative fact with the federal claims. Specifically, Fortinet asserts that the fact that the claim arose as a result of the patent dispute is insufficient for supplemental jurisdiction and that the tortious interference claim is otherwise unrelated to the patents. Mot. at 34–35. Fortinet also points out that the statement regarding financial insolvency does not relate to the alleged patent infringement. *Id.* Forescout contends that the tortious interference claim depends on the proof of the falsity of the infringement claim—a substantial question of federal patent law—and therefore must be brought in federal court. *See* Opp'n at 35.

Courts have previously found federal jurisdiction for tortious interference claims based on related issues of patent infringement, finding that the claims "form part of the same case or controversy." *See, e.g.*, *Mikohn Gaming Corp. v. Acres Gaming, Inc.*, 165 F.3d 891, 894 (Fed. Cir. 1998) (finding that the district court had jurisdiction for the interference claim under § 1338 and § 1367). *Additive Controls*, while not a tortious interference case, also concerned a patent dispute in which the defendant asserted a counterclaim of business disparagement when the plaintiff sent letters to the defendant's current and potential customers that warned them about its alleged patent infringement. *Additive Controls*, 986 F.2d at 477. The Federal Circuit found it proper that the business disparagement claim was removed to federal court, as it depended upon a substantial question of patent law. *Id.* at 478–79 ("[The] allegedly disparaging statement was its accusation that [the plaintiff] infringed the . . . patent. To prove this aspect of its case (falsity), [the plaintiff] must show that its product does not infringe the . . . patent.").

District courts have found that "claims aris[ing] out of the same dispute over the . . . patent" are sufficient for supplemental jurisdiction over tortious interference claims because "[t]he question of the patents' validity []provides the 'common nucleus of operative fact' essential to the determination of both [the plaintiff's patent] claims in this suit and [the defendant's] counterclaim [of tortious interference]." *Tools Aviation, LLC v. Digital Pavilion Elecs. LLC*, No.

20-CV-02651-PKCVMS, 2021 WL 4340949, at *4 (E.D.N.Y. Sept. 23, 2021) (finding jurisdiction because the claim "involve[d] the question of whether [the p]laintiff has validly asserted infringement of its patents or, as [the d]efendants contend, used the prospect of an infringement suit to threaten [the d]efendants' business partners."); *see also Clear Lam Packaging, Inc. v. Rock-Tenn Co.*, No. 02 C 7491, 2003 WL 22012203, at *2–3 (N.D. Ill. Aug. 22, 2003) (declining to dismiss a tortious interference claim for lack of subject matter jurisdiction because, among other reasons, "all the claims arise out of the same dispute over the . . . patent and therefore derive 'from a common nucleus of operative fact.'").

Like *Additive Controls* and *Tools Aviation*, the tortious interference claim in this case involves a statement that implicates Fortinet's right to assert infringement, which raises questions of patent validity and infringement. The communications are not tortious if it asserts a valid patent right. Whether Fortinet has valid patent rights related to the patents at issue and their potential infringement are questions of patent law.

As Fortinet's right to relief involves the resolution of a substantial question of patent law, Forescout's patent and tortious interference claims arise in the same "nucleus of operative fact." Although Forescout attempts to argue that some of Fortinet's statements were beyond assertions of patent rights, whether such statements were "far in excess of accurate notification of [the plaintiff's] patent rights" in bad faith goes to the merits of the claim, not subject matter jurisdiction. *See Clear Lam Packaging, Inc.*, 2003 WL 22012203, at *2–3 (finding subject matter jurisdiction and thereafter discussing whether defamatory statements regarding the plaintiff's "stability and ability to meet customer needs" supported an allegation of bad faith). Thus, the Court declines to dismiss the tort claim for lack of subject matter jurisdiction.

2. Preemption

The Supremacy Clause of the U.S. Constitution states that "the Laws of the United States . . . shall be the supreme Law of the Land[.]" U.S. Const. Art. VI, cl. 2. The Supremacy Clause preempts state law by means of express preemption, field preemption, or conflict preemption. *See English v. Gen. Elec. Co.*, 496 U.S. 72, 78–79 (1990). Federal patent law does not provide explicit preemption. *Id.* at 1332; 35 U.S.C. §§ 1–376 (2000). *See also Dow Chemical Co. v.*

Exxon Corp., 139 F.3d 1470, 1473–75 (Fed. Cir.1998). The Federal Circuit has explained that conflict preemption, not field preemption, is used to preempt state law with patent law. *See Hunter Douglas, Inc. v. Harmonic Design, Inc.*, 153 F.3d 1318, 1335 (Fed. Cir. 1998) (*overruled on other grounds by Midwest Indus., Inc. v. Karavan Trailers, Inc.*, 175 F.3d 1356 (Fed. Cir.1999) ("[C]onflict preemption is a more precise means of determining which state law causes of action are preempted than the blunt tool of field preemption."). Conflict preemption occurs in two ways: "when it is impossible for a private party to comply with both state and federal requirements . . . or when state law 'stands as an obstacle to the accomplishment and execution of the full purposes and objectives of Congress[.]'" *Hunter Douglas*, 153 F.3d at 1332 (quoting *Hines v. Davidowitz*, 312 U.S. 52, 67 (1941)). The Federal Circuit has noted the "essential criteria" for determining whether there is such conflict preemption considers the "objectives of the federal patent laws":

> First, patent law seeks to foster and reward invention; second it promotes disclosure of inventions to stimulate further innovation and to permit the public to practice the invention once the patent expires; third, the stringent requirements for patent protection seek to assure that ideas in the public domain remain there for the free use of the public.

153 F.3d at 1333; *see also Dow Chemical*, 139 F.3d at 1473–74.

The court must assess whether the alleged tortious conduct to determine whether "a state law tort, 'as-applied,' conflicts with federal patent law." *Id.* at 1335–37 (finding that this conduct-based approach is in harmony with the Federal Circuit's obstacle preemption in *Dow Chemical*). Under this formulation, "if a plaintiff bases its tort action on conduct that is protected or governed by federal patent law, then the plaintiff may not invoke the state law remedy, which must be preempted for conflict with federal patent law. Conversely, if the conduct is not so protected or governed, then the remedy is not preempted." *Id.*

As part of federal patent law, the Federal Circuit has "uniformly upheld a patentee's right to publicize the issuance of patents and to so inform potential infringers." *Mikohn Gaming Corp*, 165 F.3d at 897. Federal patent law contemplates this right to notice "to inform a potential infringer of the existence of the patent, whereby the recipient of the information may adjust its activities, perhaps seek a license, or otherwise act to protect itself." *Id.*; *Hunter Douglas*, 153 F.3d

at 1336. "Indeed, [the statute] . . . makes marking or specific notice of the patent to the accused infringer a prerequisite to the recovery of damages." *Id.* "Patents would be of little value if infringers of them could not be notified of the consequences of infringement, or proceeded against in the courts. Such action . . . cannot be said to be illegal." *800 Adept, Inc. v. Murex Sec., Ltd.*, 539 F.3d 1354, 1369 (Fed. Cir. 2008) (citing *Virtue v. Creamery Package Mfg. Co.*, 227 U.S. 8, 37–38 (1913)). Therefore, preventing notice of patent rights, including the publication of the patents and assertions of infringement, would be contrary to the purposes and objectives of patent law to reward invention through allowing the patentholders to assert such rights. Further, the Federal Circuit explained:

> The propriety of that notice depends on patent law and the patent issues to which the notice pertains. National uniformity, in confluence with the national scope of the patent grant and the general federal exclusivity in patent causes, require that determination of the propriety of [the plaintiff's] actions in giving notice of its patent rights is governed by federal statute and precedent and is not a matter of state tort law.

Mikohn Gaming Corp., 165 F.3d at 896. Therefore, "federal patent law bars the imposition of liability for publicizing a patent in the marketplace unless the plaintiff can show that the patentholder acted in bad faith." *Id.*

As federal patent law preempts state-law tort liability for good faith conduct in communications asserting patent infringement and potential litigation, state-law tort claims survive only if it is based on "a showing of 'bad faith' action in asserting infringement[.]" *Globetrotter Software, Inc. v. Elan Computer Grp., Inc.*, 362 F.3d 1367, 1374 (Fed. Cir. 2004); *Zenith Elecs. Corp. v. Exzec, Inc.*, 182 F.3d 1340, 1355 (Fed. Cir. 1999). Patent law "recognizes a presumption that the assertion of a duly granted patent is made in good faith"; therefore, the party arguing against the preemption has the burden of proving bad faith. *Id.* at 1374–77 ("[T]o avoid preemption, bad faith must be alleged and ultimately proven, even if bad faith is not otherwise an element of the tort claim.") (internal quotation marks omitted); *800 Adept, Inc*, 539 F.3d at 1370 ("[A] party attempting to prove bad faith on the part of a patentee enforcing its patent rights has a heavy burden to carry.").

In sum, to determine whether the tortious interference claim is preempted, a two-part

examination is relevant. First, the court determines whether Fortinet's alleged conduct falls within the scope of protection of patent rights—*i.e.,* whether the communications served to notify potential infringers of the patents or went beyond such notification. If the conduct was beyond the scope of a patent right, such conduct is not protected and therefore cannot be a basis for preemption. If the conduct was within the scope of patent rights, the Court must then proceed to the next step to determine whether preemption applies. The second step considers whether the conduct was made in bad faith. In this case, Forescout has the burden of alleging and proving bad faith.

a. Scope of Patent Rights

Fortinet contends that its actions were proper because statements informing others in the industry of a party's infringement claims are protected and therefore preempted by patent law. Further, Fortinet asserts that it has the right to notify users of Forescout's products as the users are also potential direct infringers and should be informed of the risk of an injunction. Reply at 17 (citing *Globetrotter*, 362 F.3d at 1374). Forescout argues that Fortinet's wrongful conduct went "far beyond the protected activity of simply notifying a party of potential patent infringement." Opp'n at 1.

As Forescout argues, Fortinet's communications include both assertions of patent infringement and other statements unrelated to a patentee's right to publicize the "issuance of patents and to so inform potential infringers." *Mikohn Gaming Corp*., 165 F.3d at 897. Therefore, a statement-by-statement examination of Fortinet's communications is warranted in order to assess whether Fortinet's communications are protected by patent law and fall under preemption.

Fortinet's email reads that its purpose was "to insure [Forescout's customers that they] were aware of the ongoing legal problems and future of Forescout" and proceeds to inform the readers that "Fortinet has filed lawsuit against Forescout for patent infringement related to technology held within FortiNAC." Such statements relate to Fortinet's assertion of patent infringement. They "inform potential infringers" —the users of the infringing product—of their patent right and the impending litigation within the rights of the patentee. *See* 35 U.S.C.A. § 271(a); *Judkins v. HT Window Fashions Corp.*, 514 F. Supp. 2d 753, 765 (W.D. Pa. 2007), *aff'd*

sub nom. Judkins v. HT Window Fashion Corp., 529 F.3d 1334 (Fed. Cir. 2008) (noting that while customers are rarely sued, "[they] are nonetheless infringers, and therefore, plaintiff is within his rights to inform them of possible infringement of his patent."). Therefore, these statements fall squarely within Fortinet's patent rights and a state tort claim precluding this right would conflict with the purposes and objectives of federal patent law.

Fortinet's statement to CRN that Forescout's "wrongful incorporation" of its patents "is material and goes to the heart of Fortinet's business" is also an assertion of patent infringement protected by patent law. Fortinet had the right to publicize its statement to the press, to inform potential users of the products and the marketplace, in order to publicize its patents and warn potential users that using the products would constitute infringement. *See Hunter Douglas*, 153 F.3d at 1336; *see also Mikohn Gaming Corp.*, 165 F.3d at 897.

Similarly, the statement to CRN that Fortinet "doesn't take litigation lightly and has only engaged in lawsuits to protect its intellectual property on seldom occasions when it is left no alternative" informs Forescout and relevant parties of the litigation and communicates Fortinet's belief that they have a robust case. Such statements regarding the strength of the patent are relevant to the purpose of notifying potential infringing users so that they can determine their response to the assertion of infringement, and therefore fall under Fortinet's patent rights. *See Globetrotter*, 362 F.3d at 1374.

On the other hand, Fortinet's statement that Forescout was left "on uncertain ground financially" does not assert a patent right nor advance any of the objectives of patent law, and therefore falls outside the governance of patent law. As such, tort claims based on extraneous statements about Forescout's financial situation do not obstruct the objectives of patent law, and the Court finds these statements not preempted. However, the aforementioned statements asserting Fortinet's patent rights must proceed to the next step of the analysis, and Forescout must show bad faith regarding these statements to survive preemption.

b. Bad Faith

The bad faith standard has objective and subjective components. *Golan v. Pingel Enter., Inc.*, 310 F.3d 1360, 1371 (Fed. Cir. 2002). The objective component requires a showing that the

infringement allegations are "objectively baseless." *Id.* (citing *Globetrotter*, 362 F.3d at 1375). The subjective component relates to a showing that the patentee demonstrated subjective bad faith in enforcing the patent. *Globetrotter*, 362 F.3d at 1370. A party claiming bad faith patent enforcement "must present affirmative evidence sufficient for a reasonable jury to conclude that the patentee acted in bad faith, in light of the burden of clear and convincing evidence that will adhere at trial." *Springs Window Fashions LP v. Novo Indus., L.P.*, 323 F.3d 989, 999 (Fed.Cir.2003); *Golan v. Pingel Enter., Inc.*, 310 F.3d 1360, 1371 (Fed.Cir.2002).

c. Objective Bad Faith

In order to ascertain whether Fortinet's infringement allegations were made in "bad faith," the trial court is required to determine whether those allegations were objectively baseless. *Globetrotter,* 362 F.3d at 1375. Objective baselessness can be established if the patents at issue are "obviously invalid or plainly not infringed." *Id.; see also Zenith,* 182 F.3d at 1354 ("Obviously, if the patentee knows that the patent is invalid, unenforceable, or not infringed, yet represents to the marketplace that a competitor is infringing the patent, a clear case of bad faith is made out."). This requires a showing that "the infringement allegations [were] such that no reasonable litigant could reasonably expect success on the merits." *Dominant Semiconductors Sdn. Bhd. v. OSRAM GmbH*, 524 F.3d 1254, 1260 (Fed. Cir. 2008); *800 Adept*, 539 F.3d at 1370 (citing *Pro. Real Est. Invs., Inc. v. Columbia Pictures Indus., Inc.,* 508 U.S. 49, 50 (1993) ("[T]he issue is whether the evidence was such that [defendant] could not have had a reasonable basis for believing that the patent was valid when it asserted the patent against [plaintiff's] customers."); *see also Mikohn Gaming Corp.*, 165 F.3d at 897 ("Federal precedent is that communications to possible infringers concerning patent rights is not improper if the patentholder has a good faith belief in the accuracy of the communication.").

Of the numerous arguments Forescout makes in support of finding objective baselessness, the most notable is that Fortinet "knew, or should have known, [the asserted patents] were invalid and/or not infringed by Forescout." Opp'n at 1. Forescout asserts that patents are invalid under § 101 and because of prior art, including the accused product itself. Opp'n at 29 (citing *Nuance Commc'ns, Inc. v. MModal LLC*, No. 17-1484-MN-SRF, 2018 WL 6804488, at *4 (D. Del. Dec.

27, 2018) (denying the Rule 12 motion because "[the counterclaimant] identifie[d] numerous specific prior art references under §§ 102 and 103 purporting to show that [the plaintiff] ha[d] no basis for alleging the Asserted Patents [were] valid and enforceable."). Forescout also notes that the question of bad faith is a factual contest and cannot be resolved on a motion to dismiss. Opp'n. at 33. Fortinet argues that Forescout did not meet the high bar of showing bad faith and failed to sufficiently plead that Fortinet's infringement lawsuit is objectively unreasonable. Mot. at 31–34. Indeed, it is true that bad faith is a high bar that must be found by clear and convincing evidence. *Zenith*, 182 F.3d at 1352; *800 Adept*, 539 F.3d at 1370 (The "party attempting to prove bad faith on the part of a patentee enforcing its patent rights has a heavy burden to carry."). Fortinet also notes that patents are entitled to a presumption of validity. Mot. at 32.

The Court finds that it is premature to determine the question of bad faith at this stage. First, the question of patent validity is "open to reasonable debate at this point." As Fortinet argues, the Court finds that there is no obvious invalidity under § 101 in light of the uncertainty discussed in sections above as to how *Alice* applies to the patents in question. Nor can the Court determine at this stage whether Forescout's assertions of the patent's invalidity for anticipation and obviousness under §§ 102 and 103 are so obvious that Fortinet could not have "realistically expected success on the merits at the time the suit was filed." *Hoffman-La Roche Inc. v. Genpharm Inc.*, 50 F. Supp. 2d 367, 380 (D.N.J. 1999). On the other hand, Forescout specifically identifies numerous prior art that purports to anticipate or render obvious the patents at issue, as well as their exemplary combinations. Docket No. 107-1 at 7–10; Docket No. 107-2 at 7–10. That identification is sufficient to meet the plausibility requirement at this stage. *See, e.g.*, *Nuance Commc'ns, Inc.*, 2018 WL 6804488, at *4 ("MModal identifies numerous specific prior art references under §§ 102 and 103 purporting to show that Nuance has no basis for alleging the Asserted Patents are valid and enforceable. Consequently, MModal meets the standard of plausibility required at the 12(b)(6) stage.") (citation omitted). Therefore, Forescout's pleadings "adequately allege bad faith by pointing to a specific basis" for its allegations. *Id.*; *Indect USA Corp. v. Park Assist, LLC*, No. 3:18-CV-02409-BENMDD, 2019 WL 3780274, at *8 (S.D. Cal. Aug. 12, 2019).

Second, the Court must also consider whether there was a basis for Fortinet to reasonably believe that Forescout infringed its patents. *800 Adept, Inc.*, 539 F.3d at 1371. However, Forescout alleges nothing about whether Fortinet undertook a reasonable investigation regarding the infringement. *Cf. Sandisk Corp. v. LSI Corp.*, No. C 09-02737 WHA, 2009 WL 3047375, at *3 (N.D. Cal. Sept. 18, 2009) (dismissing the plaintiff's claim when the plaintiff alleged that the defendant "knew or should have known its allegations of infringement were false" but failed to provide any specific facts to support such an assertion and because the defendant had analyzed and determined that plaintiff's products infringed). "The resolution of the question whether plaintiffs' suit is objectively baseless . . . involves the determination of whether plaintiffs undertook a reasonable investigation before filing suit, whether plaintiffs knew or should have known that [Forescout] had not infringed the [Fortinet] patents, and whether a reasonable litigant could have realistically expected success on the merits at the time the suit was filed." *Id.* Reasonableness is a generally question of fact; the Court cannot at this juncture determine whether there was objective bad faith.

Therefore, because the questions of patent validity and infringement are not obvious, it is premature to determine the question of objective bad faith at this stage of the litigation.

d. Subjective Bad Faith

Finding subjective bad faith is primarily concerned with the parties using litigation as a weapon when it is a mere "sham"; therefore, the subjective prong of this test looks to the "subjective expectation of success" in the underlying litigation. *Pro. Real Est. Invs.*, 508 U.S. at 57. For example, accusing a competitor of patent infringement for an invalid patent and never actually filing the infringement suit shows that there was never any subjective expectation of success. In such cases, the patent infringement action is used merely as a weapon. *Globetrotter*, 362 F.3d at 1375. Subjective bad faith focuses on "whether the baseless lawsuit conceals an attempt to interfere directly with the business relationships of a competitor." *Nuance Commc'ns, Inc.*, 2018 WL 6804488, at *3 (internal quotation marks omitted). This includes the history of bringing patent infringement suits against its market competitors as a predicate to acquiring them, threats to sue as retribution for a failure to sell, dissemination of misleading press release with

false accusations of patent infringement, never actually filing an infringement lawsuit, the timing of communications alleging infringement, or inadequate investigation. *Id.*; *Globetrotter*, 362 F.3d at 1375; *Dominant Semiconductors*, 524 F.3d at 1264; *Well Master Corp. v. Luckyshot LLC*, No. 19-CV-01617-CMA-STV, 2019 WL 11314994, at *3 (D. Colo. Dec. 10, 2019).

In its motion to dismiss, Fortinet does not meaningfully engage with the subjective bad faith analysis and acknowledges that it focused its briefing on the objective prong. Mot. at 31, n4. Fortinet is correct that "[a]n objectively reasonable effort to litigate "cannot be [a] sham regardless of subjective intent." *Globetrotter*, 362 F.3d at 1375–76 (quoting *Pro. Real Est. Invs*, 508 U.S. at 57) ("Absent a showing that the infringement allegations are objectively baseless, it is unnecessary to reach the question of the patentee's intent."). *800 Adept*, 539 F.3d at 1370. However, the question of subjective intent remains relevant as absent a sufficient allegation of subjective bad faith, any applicable preemption cannot be overcome.

Forescout alleges that Fortinet filed its lawsuit with the intention of interfering with Forescout's corporate acquisition and customer relations. Counterclaim at 46. It reasons that Fortinet "knew or should have known" that the lawsuit was baseless, that it filed its suit one business day before the acquisition was scheduled to close, and included extraneous allegations relating to the acquisition in the Complaint. *Id.* Fortinet's knowledge or recklessness as to patent invalidity, if established, would indicate that it filed sham litigation to tortiously interfere with the competitor's business. *Conbraco Indus., Inc. v. Mitsubishi Shindoh Co.*, No. 3:14-CV-00368-RJC, 2015 WL 3506487, at *3 (W.D.N.C. Jan. 30, 2015). In light of these allegations, the truth and accuracy of which cannot yet be adjudicated, the Court cannot find that Forescout has failed to plausibly plead subjective bad faith. Accordingly, the Court cannot find preemption of Fortinet's tortious interference claim as a matter of law at this juncture.

3. Claim for Tortious Interference

Forescout asserts a claim for tortious interference. Fortinet argues that Forescout's claim fails because Forescout has not specified which form of tortious interference it claims. In California, there are two distinct forms of tortious interference: "intentional interference with contract and intentional interference with prospective economic advantage." *Korea Supply Co. v.*

Lockheed Martin Corp., 29 Cal.4th 1134, 1157 (2003). Fortinet notes that Forescout merely pleads "tortious interference with business relationships" and argues that the claim mixes the elements of the two torts, ultimately failing to plead either claim. Reply at 22.

a. Intentional Interference with Contract

Fortinet argues that a claim of intentional interference with contract fails because Forescout did not identify a specific contract. Reply at 21. Forescout contends that it has pled the essential elements of a tortious interference claim, noting that intentional interference with an existing contract is a "wrong in and of itself." *Id.* at 1158. However, no contract was identified. *Korea Supply*, 29 Cal.4th at 1157. Even assuming that the botched acquisition deal with Advent is the contractual relationship at issue, intentional inference is a tort that requires an enforceable contract, which Forescout did not have. Therefore, there is no claim of intentional interference with a specific contract. *PMC, Inc. v. Saban Ent., Inc.*, 45 Cal. App. 4th 579 (1996) ("[A] cause of action for intentional interference with contract requires an underlying enforceable contract."), *overruled on other grounds by Korea Supply*, 29 Cal.4th at 1134.

b. Intentional Interference with Prospective Economic Advantage

In California, intentional interference with prospective economic advantage has five elements: (1) the existence, between the plaintiff and some third party, of an economic relationship that contains the probability of future economic benefit to the plaintiff; (2) the defendant's knowledge of the relationship; (3) intentional acts by the defendants designed to disrupt the relationship; (4) actual disruption of the relationship; and (5) harm proximately caused by the defendant's action. *Id.* at 1153. The defendant's intentional acts must be wrongful and independently actionable by some measure beyond the interference itself. *Della Penna v. Toyota Motor Sales, U.S.A., Inc.*, 11 Cal.4th 376, 393 (1995). The tort does not punish lawful competition, choice of commercial relationships, or pursuit of commercial objectives, even if carried out with an improper motive. *Korea Supply*, 29 Cal.4th at 1158–59.

Fortinet argues that Forescout failed to adequately plead two elements of its claims. First, Fortinet states that Forescout failed to establish how Fortinet committed an independently actionable wrong. Mot. at 36. Independently actionable violations include violations of law or

unethical practices such as violence, misrepresentation, defamation, libel, or infringement. *Ingrid & Isabel, LLC v. Baby Be Mine, LLC*, 70 F. Supp. 3d 1105, 1120 (N.D. Cal. 2014). Forescout counters that there was independently actionable wrong because Fortinet's conduct included misrepresentation, defamation and unfounded litigation as its claims are objectively baseless because Fortinet knew or should have known that its claims were not infringed and were invalid or patent-ineligible. Opp'n at 36. While it is premature to determine whether Fortinet's infringement action was objectively baseless, Forescout has sufficiently pled a claim of wrong to survive a motion to dismiss. *Id.*

Second, Fortinet argues that Forescout failed to identify any particular customers it was deprived of. Mot. at 37. In order to state a claim for intentional interference with prospective business advantage, the plaintiff must allege facts showing that the defendant interfered with the plaintiff's relationship with an "identifiable buyer." *Westside Ctr. Associates v. Safeway Stores, Inc.*, 42 Cal.App.4th 507, 527 (1996). Allegations that a defendant interfered with the plaintiff's relationship with an "as yet unidentified" customer generally will not suffice. *Id.* Merely stating that an ongoing relationship with customers was harmed is conclusory and insufficiently pleaded. *Sybersound Recs., Inc. v. UAV Corp.*, 517 F.3d 1137, 1151 (9th Cir. 2008); *see also Amaretto Ranch Breedables, LLC v. Ozimals, Inc.*, 790 F. Supp. 2d 1024, 1032 (N.D. Cal. 2011). Fortinet argues that the tort requires Forescout to show that Fortinet's actions affected more than a relationship with "repeat customers." Reply at 22 (citing *Google Inc. v. Am. Blind & Wallpaper Factory, Inc.*, No. C-03-05340 JF, 2005 WL 832398, at *9 (N.D. Cal. Mar. 30, 2005) (relationship with "repeat customers who "probabl[y] will continue to seek to visit its Web site and purchase its goods and services" was too speculative and did not "rise to the level of the requisite promise of future economic advantage.")).

Forescout contends that identification of a specific customer is unnecessary, and some manner of an economic relationship is all that is required. Opp'n at 37. Forescout is correct—an identification by name is not required, just "that the defendant was aware its actions would frustrate the legitimate expectations of a specific, albeit unnamed, party." *Roy Allan Slurry Seal, Inc. v. Am. Asphalt S., Inc.*, 184 Cal. Rptr. 3d 279, 284 (Ct. App. 2015), *rev'd on other grounds*, 2

Cal. 5th 505 (2017) (citing *Ramona Manor Convalescent Hosp. v. Care Enterprises*, 177 Cal. App. 3d 1120, 1133 (Ct. App. 1986)). However, "while . . . a plaintiff need not give the name of the third-party, none of them abrogates the requirement that a plaintiff still must allege sufficient facts to allow the Court to plausibly infer some real third-party—named or unnamed—existed and expected to partake in the relationship." *Logistick, Inc. v. AB Airbags, Inc.*, No. 321-CV-00151, 2021 WL 2433944, at *5 (S.D. Cal. June 15, 2021).

Courts in this district have not found this requirement to be a high bar at the motion to dismiss stage. It is sufficient that the plaintiff plausibly alleges "specific facts putting the defendant on notice that a third-party . . . existed." *Id.* at *7. For instance, in *Code Rebel*, the Court found that alleging interference with "actual and potential customers" for a specific program to be sufficient:

> Plaintiff alleges that an economic and business relationship existed between Plaintiff and its actual and prospective customers of the iRAPP programs. Although Plaintiff does not specifically identify existing third parties with whom there was an existing economic or business relationship, Plaintiff's allegation of interference with "actual and potential customers" is sufficient to satisfy federal pleading requirements.

Code Rebel, LLC v. Aqua Connect, Inc., No. CV-13-4539, 2013 WL 5405706, at *5–7 (C.D. Cal. Sept. 24, 2013) (citation omitted).

Similarly, in *Logistick*, the defendant argued that the plaintiff failed to name its customers and to specify what actions its customers took toward purchasing the plaintiff's products. *Logistick, Inc.*, 2021 WL 2433944 at *5. The plaintiff had only argued that "it [was] evident from the [c]omplaint that these customers were consumers of [the p]laintiff's disposable load bars that compete with [the d]efendant's . . . product." *Id.* This was sufficient for the court to find that "specific facts putting the defendant on notice that a third-party, indeed, existed[,]" and therefore sufficient to pass the *Twombly/Iqbal* standard. *Id.* at *7.

Therefore, *Code Rebel* and *Logistick* suggest that while merely pointing to "customers" or "repeated customers" generally is insufficient, alleging that a relationship with customers existed for specific products is sufficient to plausibly allege that a relationship existed and pass the Rule 12(b)(6) stage. In this case, Forescout alleges that Fortinet's sample email was used to "target

folks looking at or using ForeScout." Counterclaim at 46. However, only one product, FortiNAC, is at issue and specified in the sample email. *See* Complaint at 46–47. Therefore, like the "actual and prospective customers" of iRAPP programs in *Code Rebel*, the allegation that Fortinet interfered with "current and prospective customers" of FortiNAC products is "sufficient to satisfy federal pleading requirements." *Code Rebel*, 2013 WL 5405706, at *6.

IV. CONCLUSION

For the foregoing reasons, the Court **DENIES** Fortinet's motion to dismiss.

This order disposes of Docket No. 115.

IT IS SO ORDERED.

Dated: November 29, 2021

EDWARD M. CHEN
United States District Judge

United States District Court
Northern District of California